Introduction to Cryptography

Outline

- Introduction to Cryptography and Network Security
- Security Goals
- Cryptographic attacks
- Cryptology
- Security Services
- Security Mechanism

Introduction to CRNS

- **Cryptography:**
  - It is a word with **Greek origin** whose meaning is **"hidden/secret writing".**
  - The Oxford Dictionary (2006) defines cryptography as **the art of writing or solving codes**.
  - The art and science of **keeping message secure** from others.
  - To enable two people to communicate over insecure channel in such a way that opponent cannot understand what is being said.
  - Mechanism of achieving security by **encoding/ converting the original message** into some another form in such a way that **message becomes unintelligible.**

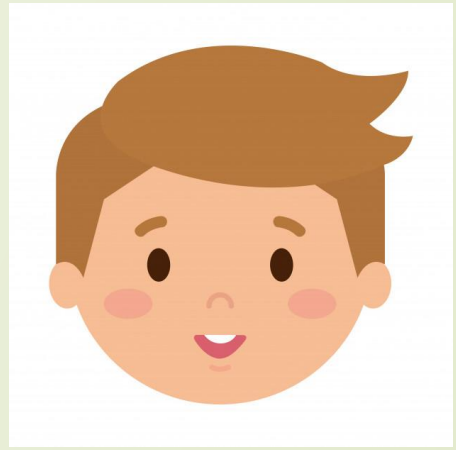
Hard to understand

Continue…

- Allows us to **scramble/descramble the text** in such a way that they would **appear meaningless.**
- To understand the Cryptography:
  - Number Theory
  - Probability

Alice

"Your Account Details
Id:xyz
Password: hellowrd"



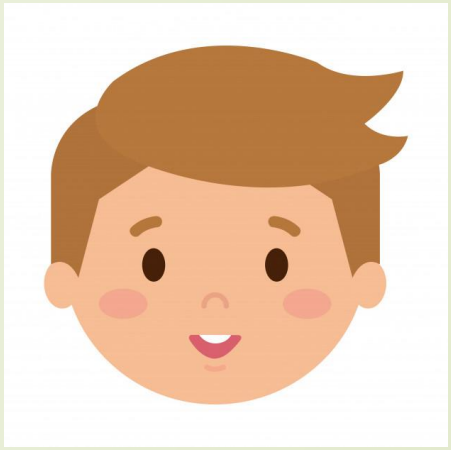
BoB

Communication without using Cryptography

Opponent

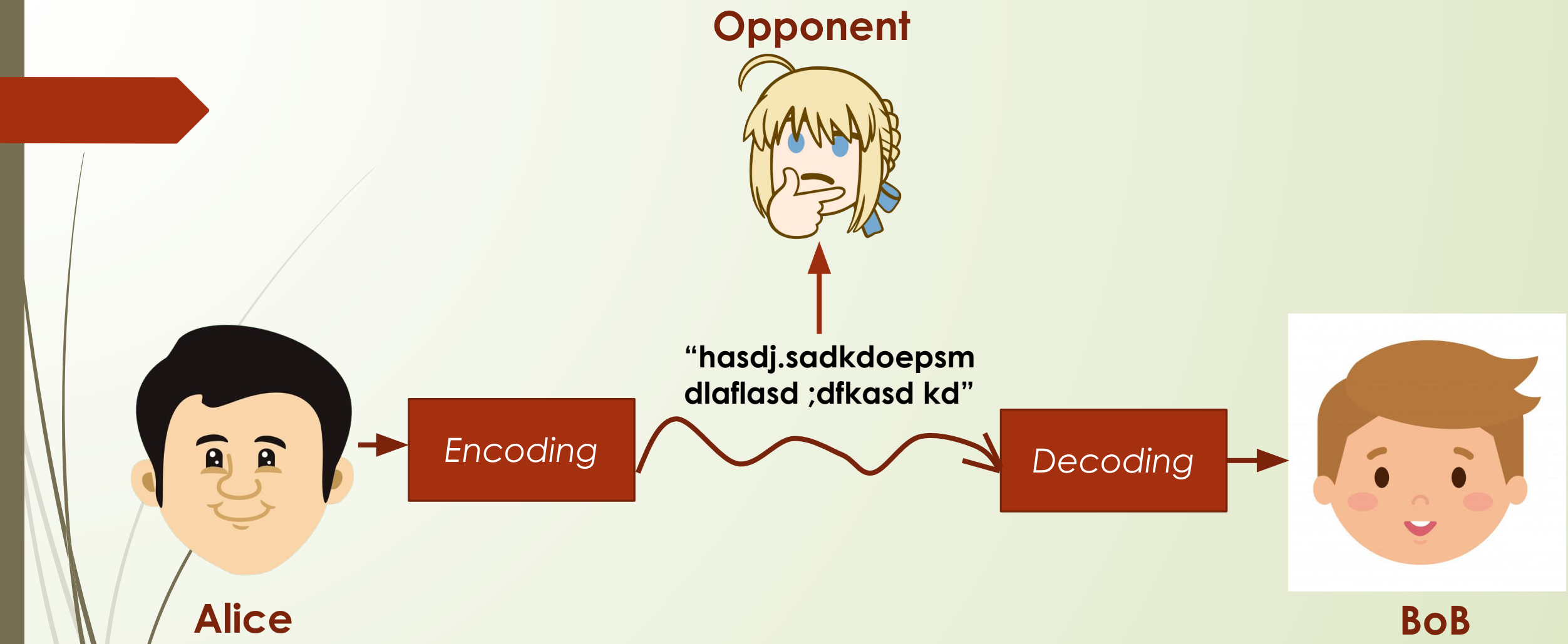
"Your Account Details
Id:xyz
Password: hellowrd"

Alice



BoB

Communication without using Cryptography

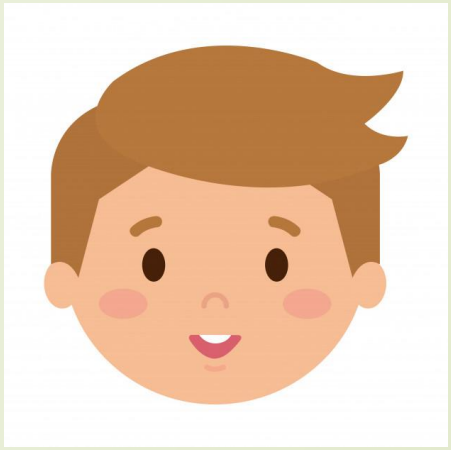


Communication with the use of Cryptography

Opponent

“hasdj.sadkdoepsm
dlaflasd ;dfkasd kd”

Alice



BoB

Communication with the use of Cryptography

Application of Cryptography

- Secure communications
- End-to-End Encryption
- Storing Data
- Storing Passwords
- Authentication/Digital Signatures
- Time Stamping
- Disk Encryption
- Electronic Money

Security Objectives/ Goals

- **Confidentiality – Information need to be hidden from unauthorized access**.
  - Sender and intended recipient should be able to access the content of the message.
  - confidentiality means something that is secret and is not supposed to be disclosed to unintended people or entities.

Continue…

- **Example (Confidentiality) :**
  - In military, concealment of sensitive information is major concern.
  - In Industry hiding some data/ Information from competitors such as tender details/new product details is critical.
  - If Alice is sending a message to Bob, it should be impossible or computationally infeasible for Eve to learn the contents of an encrypted message without knowledge of the secret key.

Continue…

- **Integrity – Protected** from **unauthorized change.**
  - When the content of the message are changed after the sender sends it and before the it reaches to the intended recipient.
- **Example (Integrity) :**
  - For example, assume that Alice encrypts a message to Bob by encoding each letter as its position in the alphabet (A=1, B=2, etc.). If Eve can intercept the message, she can modify the message without Bob knowing.

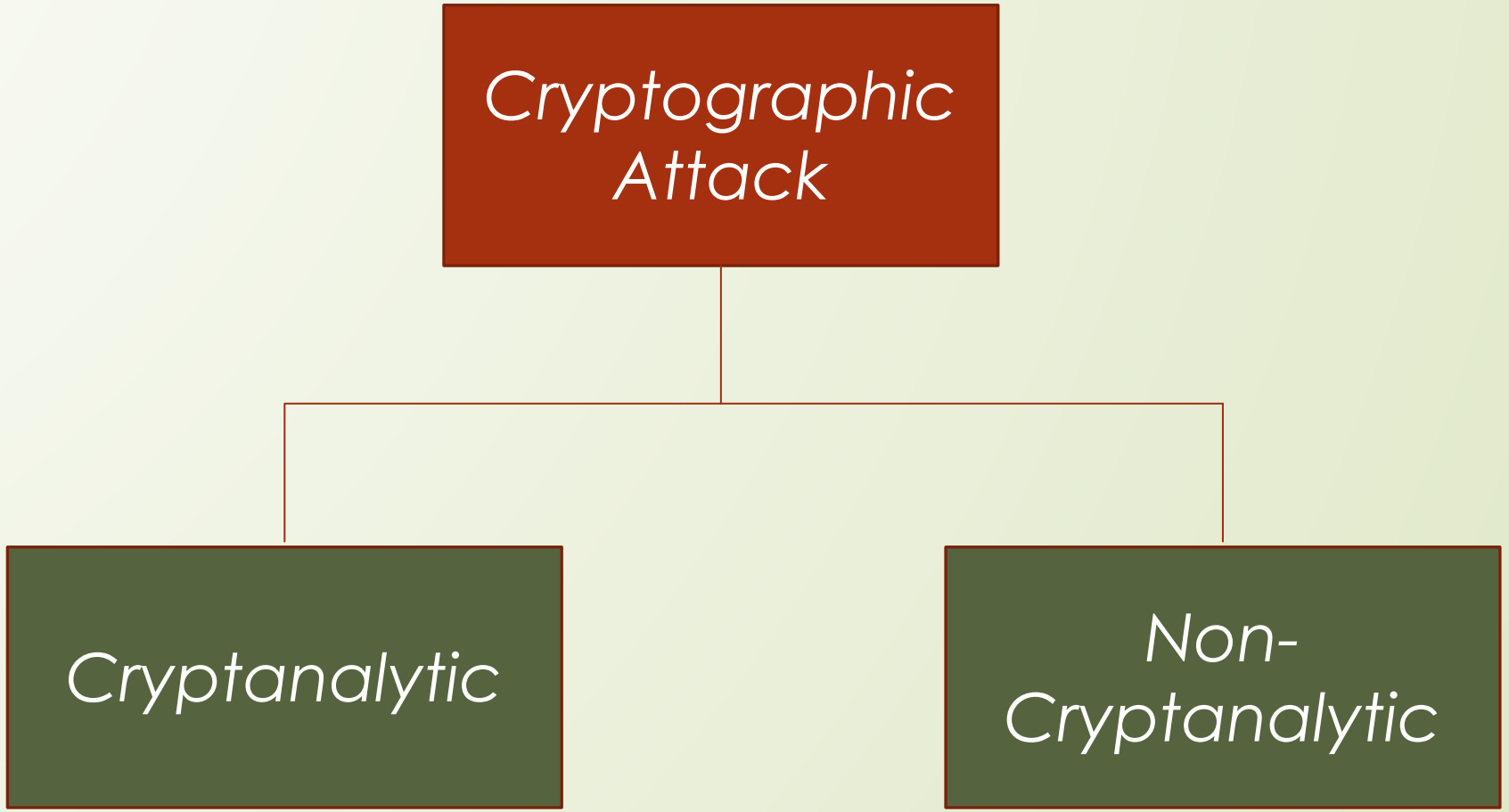
Continue…

- **Availability – Available to authorized user when it is needed.**
- **Example (Availability):**
  - You have uploaded your all-important documents on DigiLocker and at some moment the application is not accessible at the time of need due to heavy load on server.

Security attack:

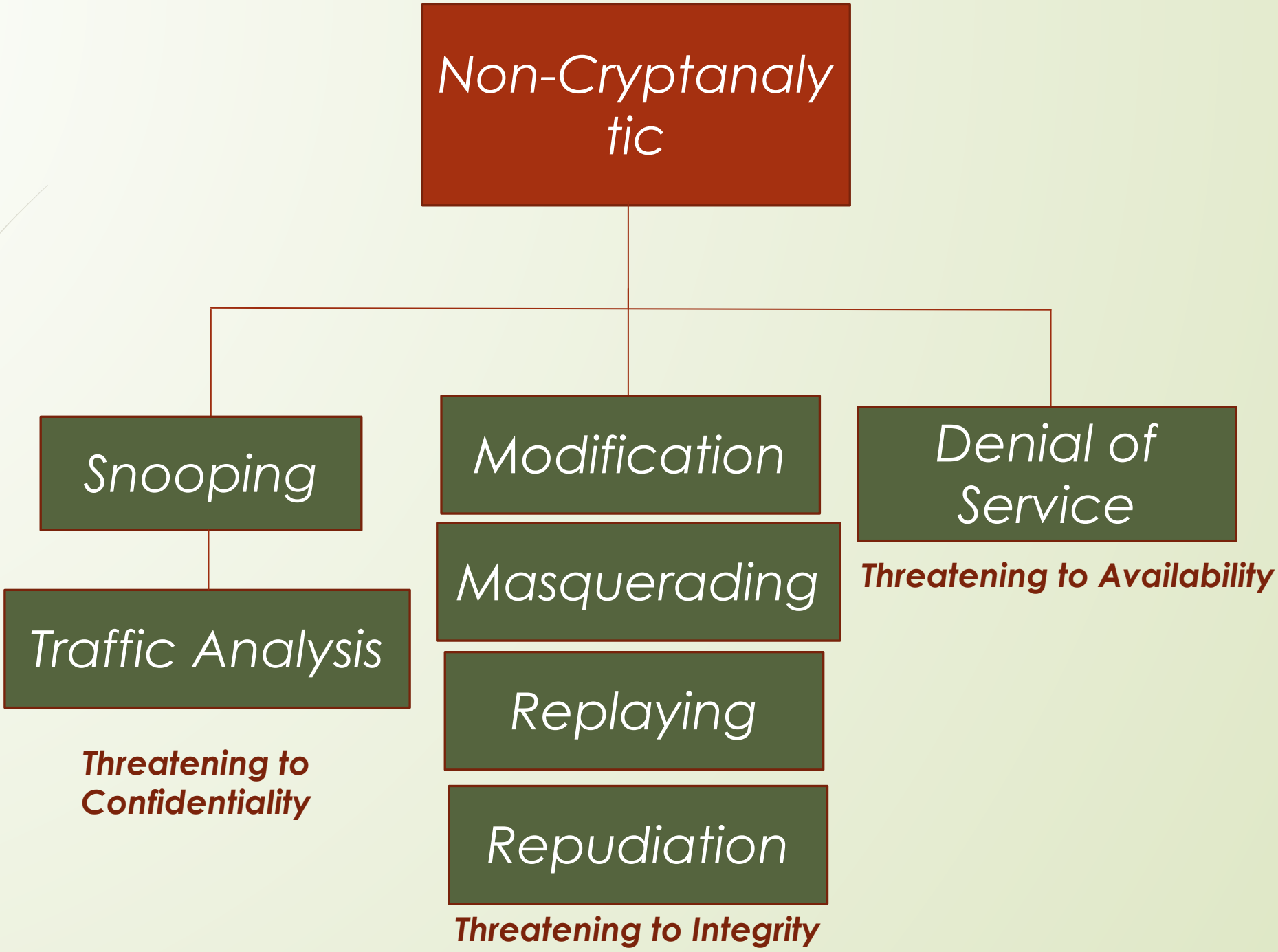
Any action that compromises the security of information owned by an organization.

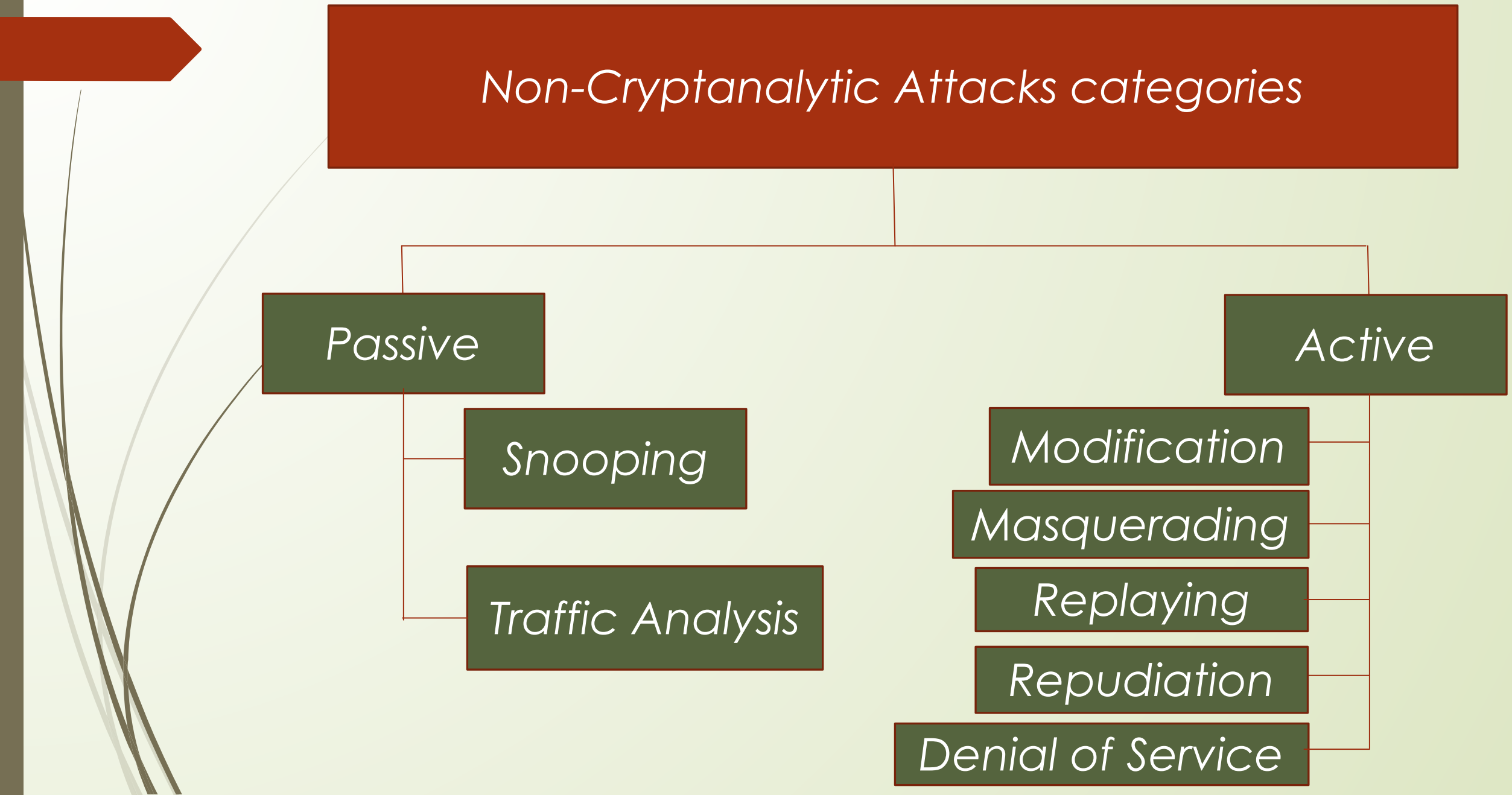
Cryptographic Attack



Cryptanalysis

- **The science of cracking codes and decoding secrets.**
- **Combination of statistical and algebraic technique to recover a message or secret key** from the decoded message **without knowing actual message, method of encoding or key**.
- It is **a technique** of **decoding messages from a unintelligible format without knowing** how they were initially converted from intelligible (understandable) format to unintelligible format.
- **Brute force attack-** Attacker tries every possible keys to recover the message.


Non-Cryptanalytic
Snooping
Traffic Analysis
Threatening to Confidentiality
Modification
Masquerading
Replaying
Repudiation
Threatening to Integrity
Denial of Service
Threatening to Availability


Non-Cryptanalytic Attacks categories
Passive
Snooping
Traffic Analysis
Active
Modification
Masquerading
Replaying
Repudiation
Denial of Service

Passive Attack

- **A passive attack** attempts to learn or make use of information from the system but does not affect system resources.
- Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions.
- The goal of the opponent is to obtain information that is being transmitted.
- Passive attacks are very difficult to detect, because they do not involve any alteration of the data.
- Typically, the message traffic is sent and received in an apparently normal fashion, and neither the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern.

Active Attack

- **An active attack** attempts to alter system resources or affect their operation.
- Whereas passive attacks are difficult to detect, measures are available to prevent their success.
- On the other hand, it is quite difficult to prevent active attacks absolutely because of the wide variety of potential physical, software, and network vulnerabilities.
- Instead, the goal is to detect active attacks and to recover from any disruption or delays caused by them. If the detection has a deterrent effect, it may also contribute to prevention.

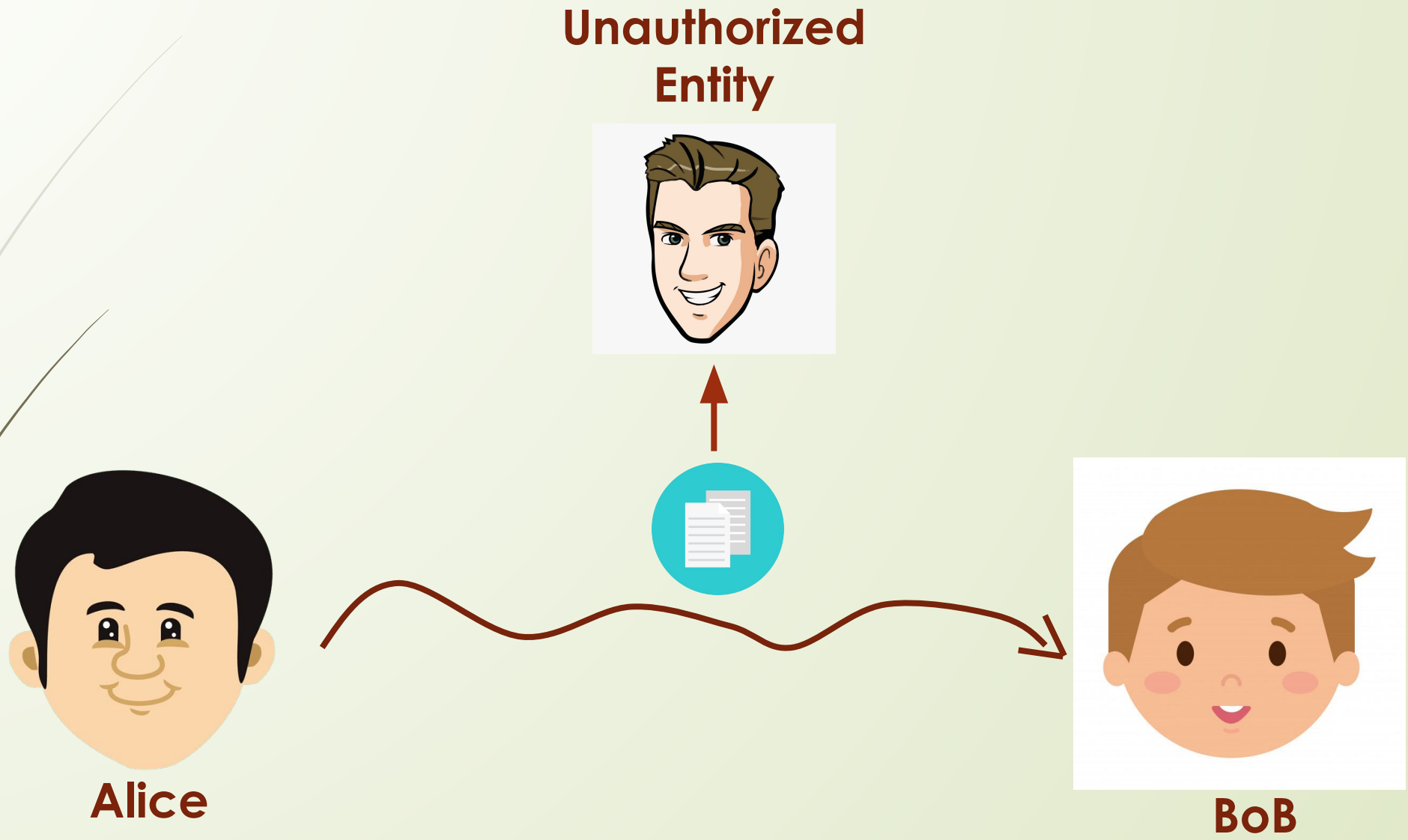
Snooping

- **Unauthorized access to** or **interception of data**.
- **Example:** a file transferred through the Internet may contain confidential information.
- An unauthorized entity may intercept the transmission and use the contents for his own benefits.
- To prevent the snooping, the data must be made non intelligible to the the interceptor by using some techniques.

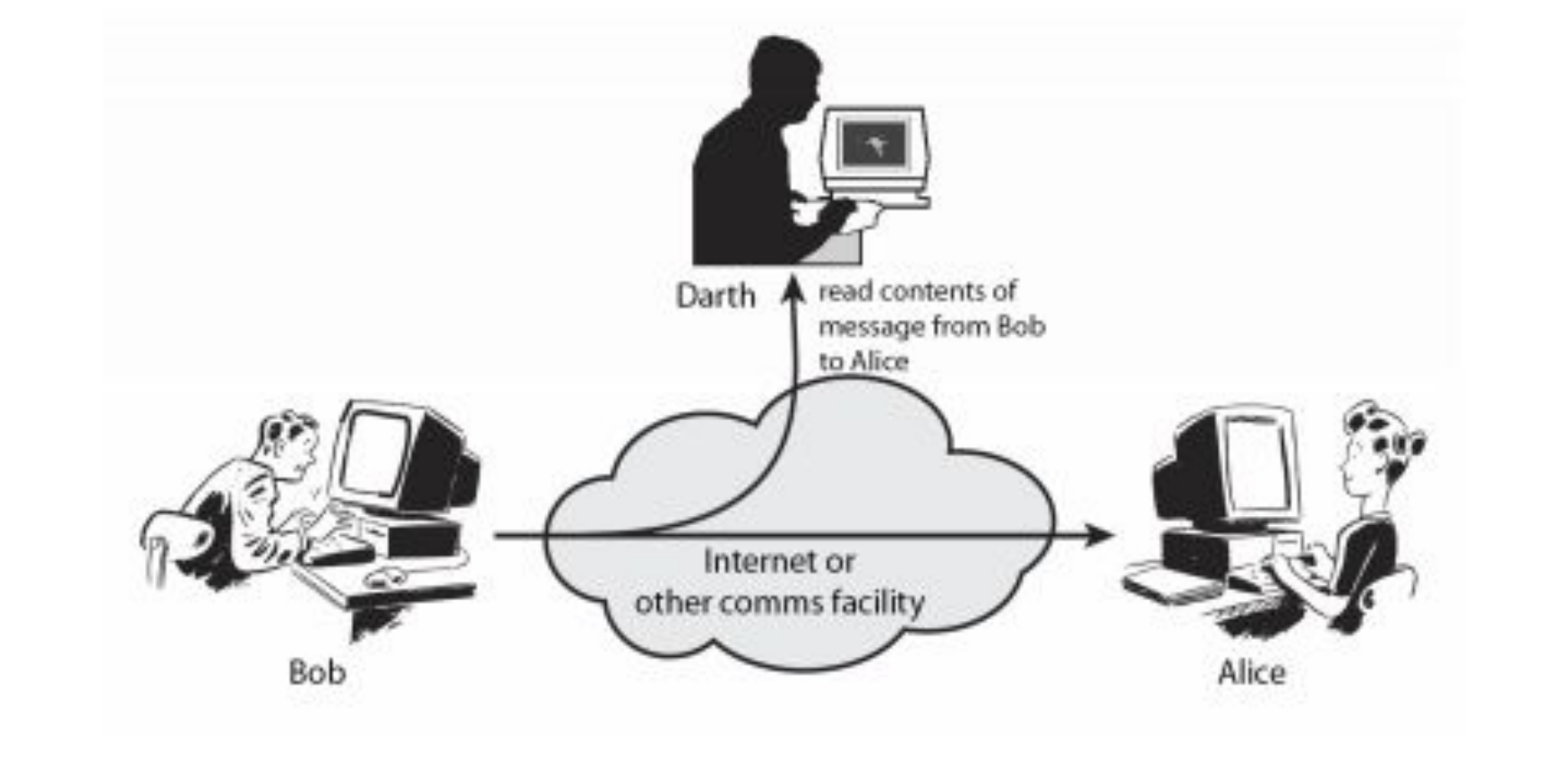
Traffic Analysis

- Although **a data is non-intelligible** for the interceptor, but he can **still extract some other type of information** by monitoring the online traffic.
- **Example:**
- Opponent can **get email ids of sender and receiver.**
- By analyzing requests and responses, **nature of the transaction can be identified.**

Continue…



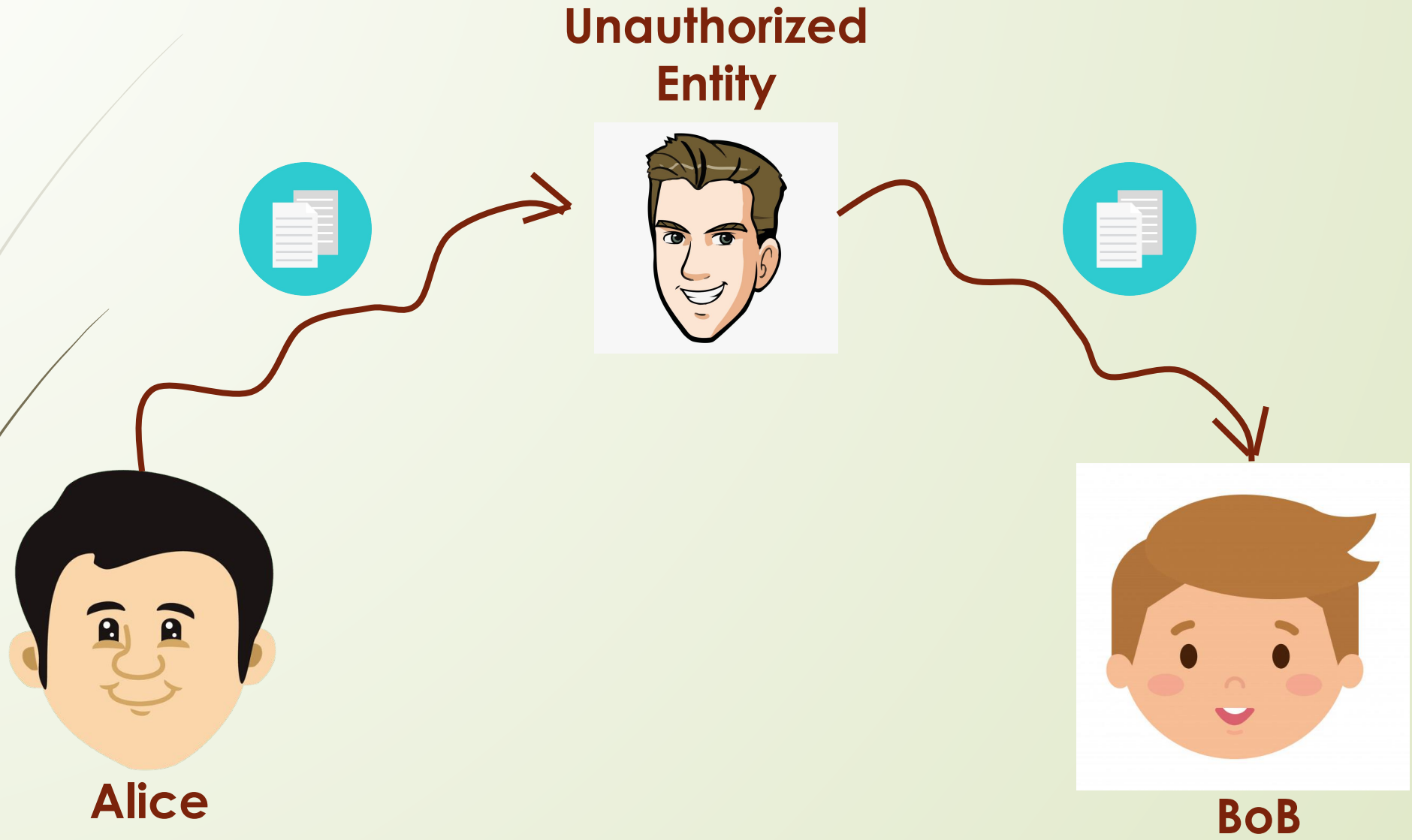
Passive Attacks
Traffic Analysis, Release of Message Content



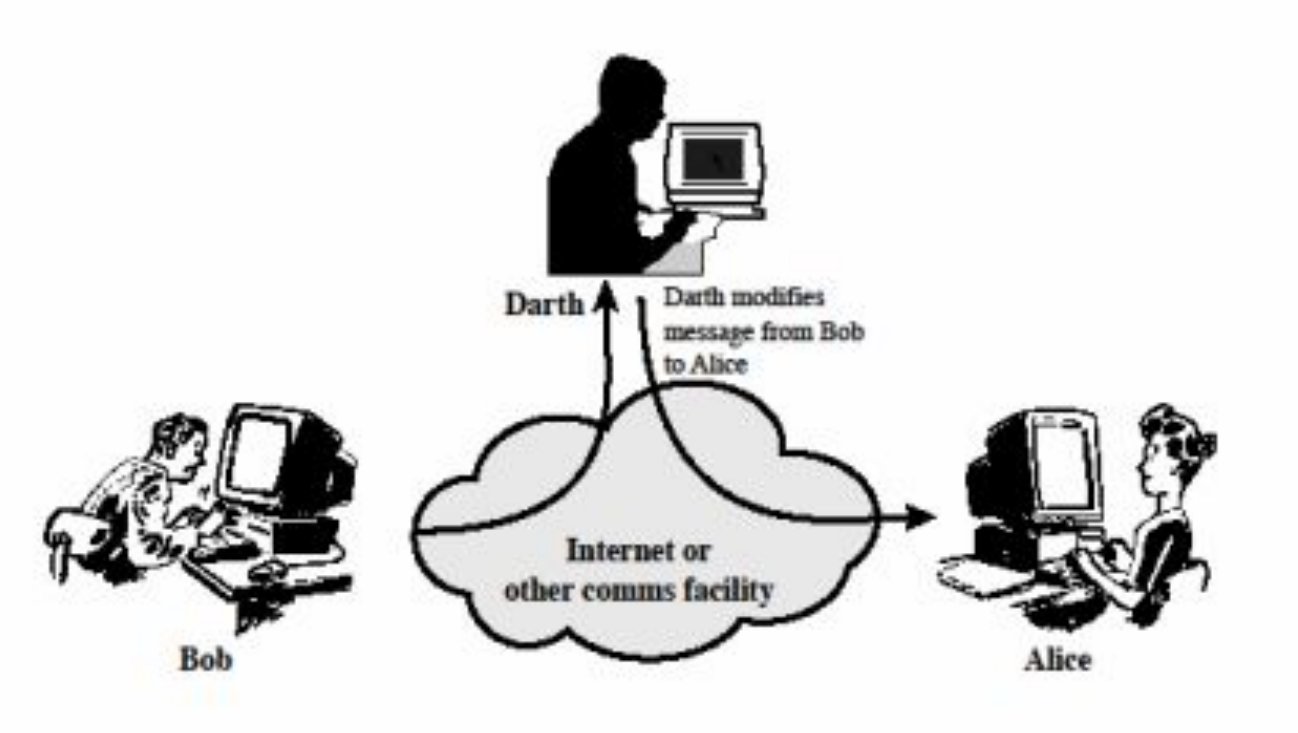
Modification

- After **incepting or accessing the information**, the attacker **modifies the information** to make it beneficial to himself and **send it to the receiver**.
- Example:
- A customer sends a message to as bank to do some transaction. The attacker intercepts the message and modifies the details of transaction to get some benefits.
- Sometime attackers simply deletes or delay the message to harm the system or reputation of the sender.

Continue…



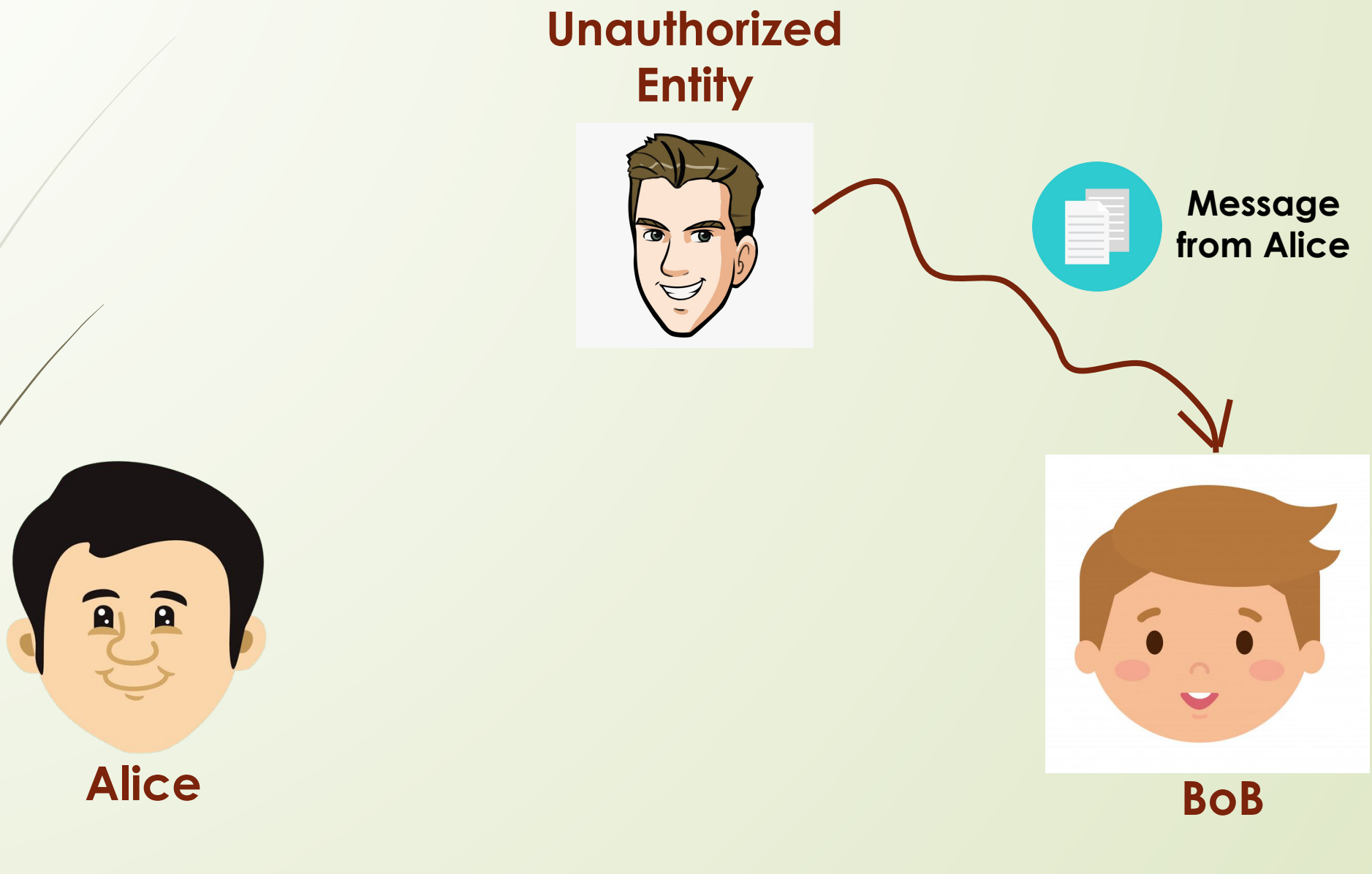
Active attack-
Modification of Message Content



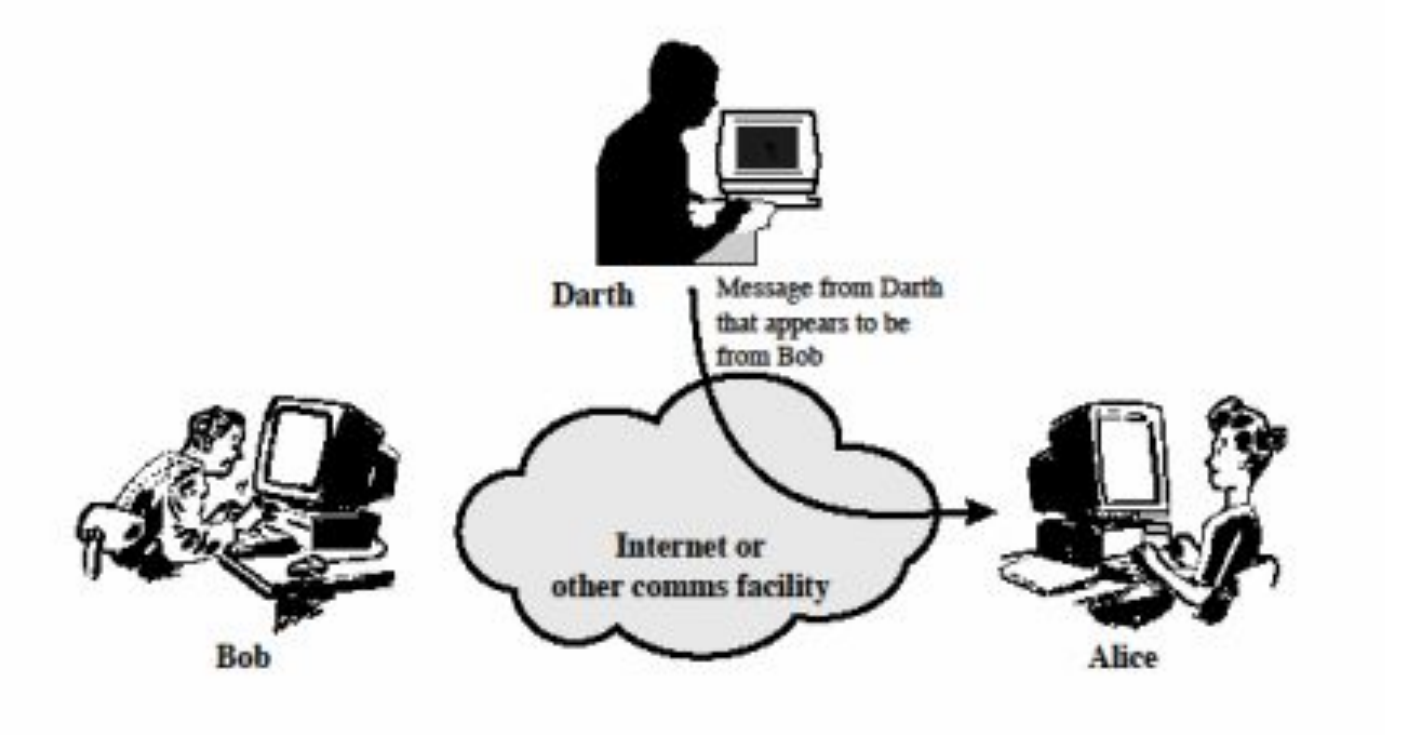
Masquerading

- Also called **spoofing.**
- The attacker **impersonates somebody else**.
- **Example:**
- Attacker may **get bank card and PIN** of the bank customer and **pretend that she is that customer.**
- A user **tries to contact bank** and **another site pretends that it is a bank** and **obtains some information** about the user.

Continue…



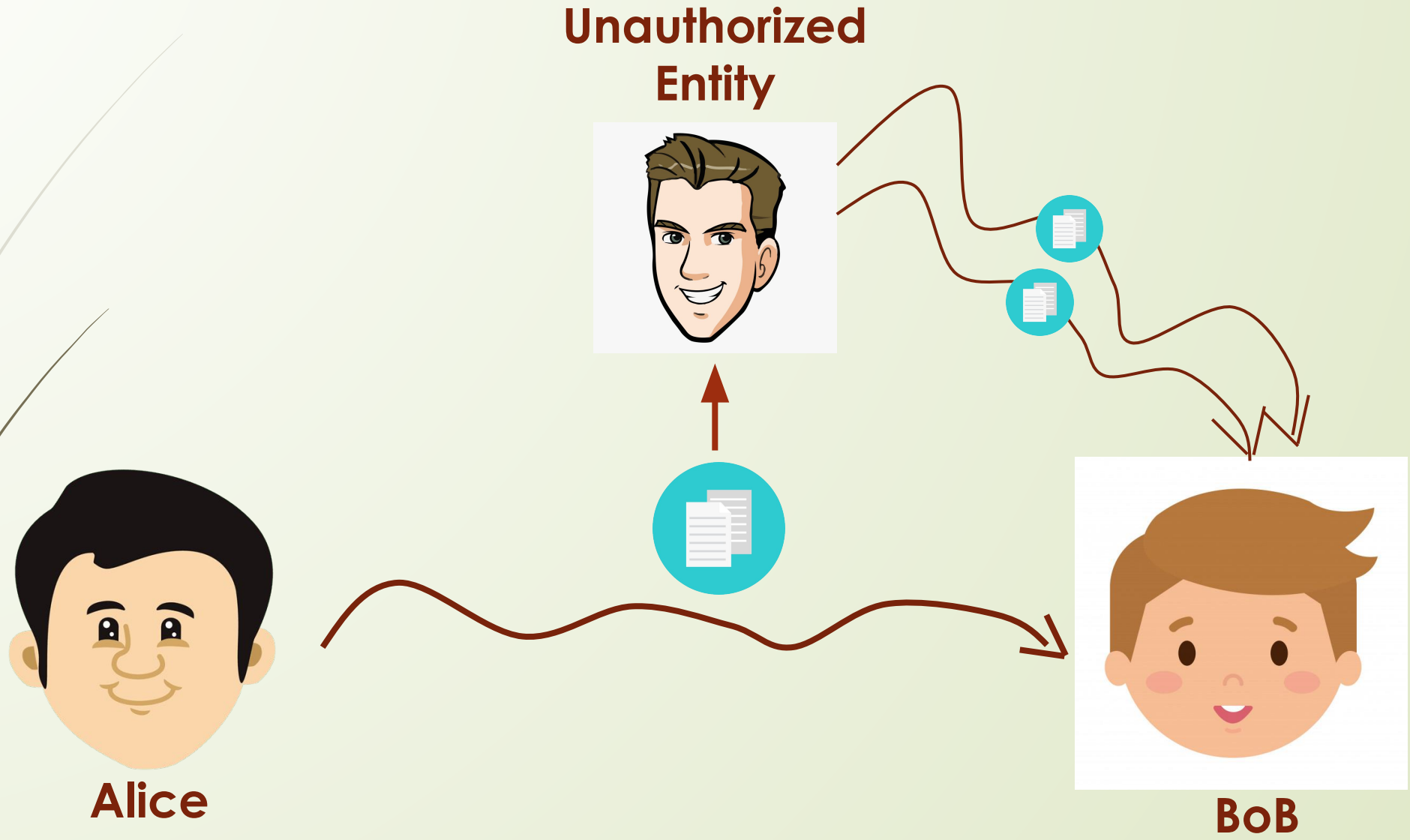
Active Attack- Masquerading



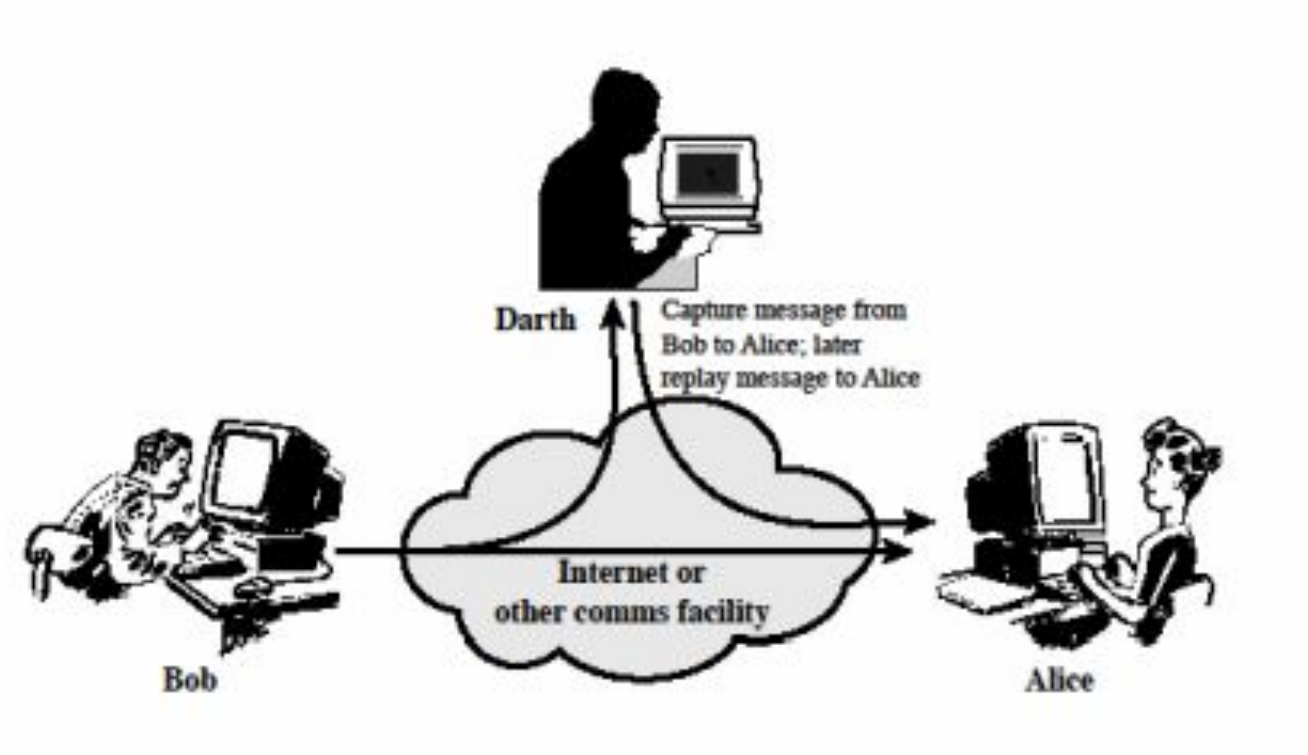
Replaying

- Obtains the copy of the message sent by the authorized user and later tries to replay it to create unauthorized effect.
- **Example:**
- A person sends a request to her bank to ask for a payment to the attacker, who has done the job for her.
- The attacker intercepts the message and send it again to receive another payment from the bank.

Continue…



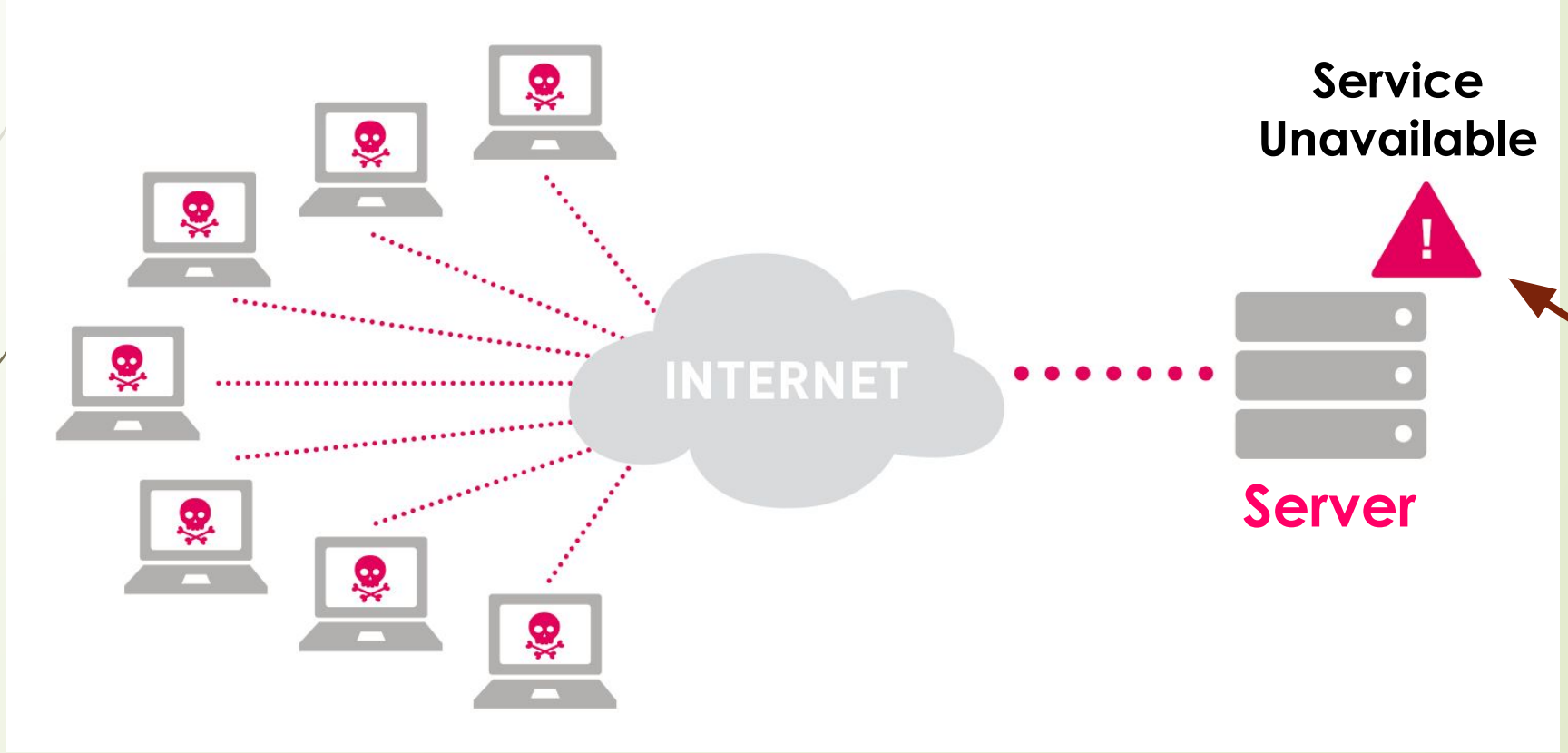
Active attack- Replay



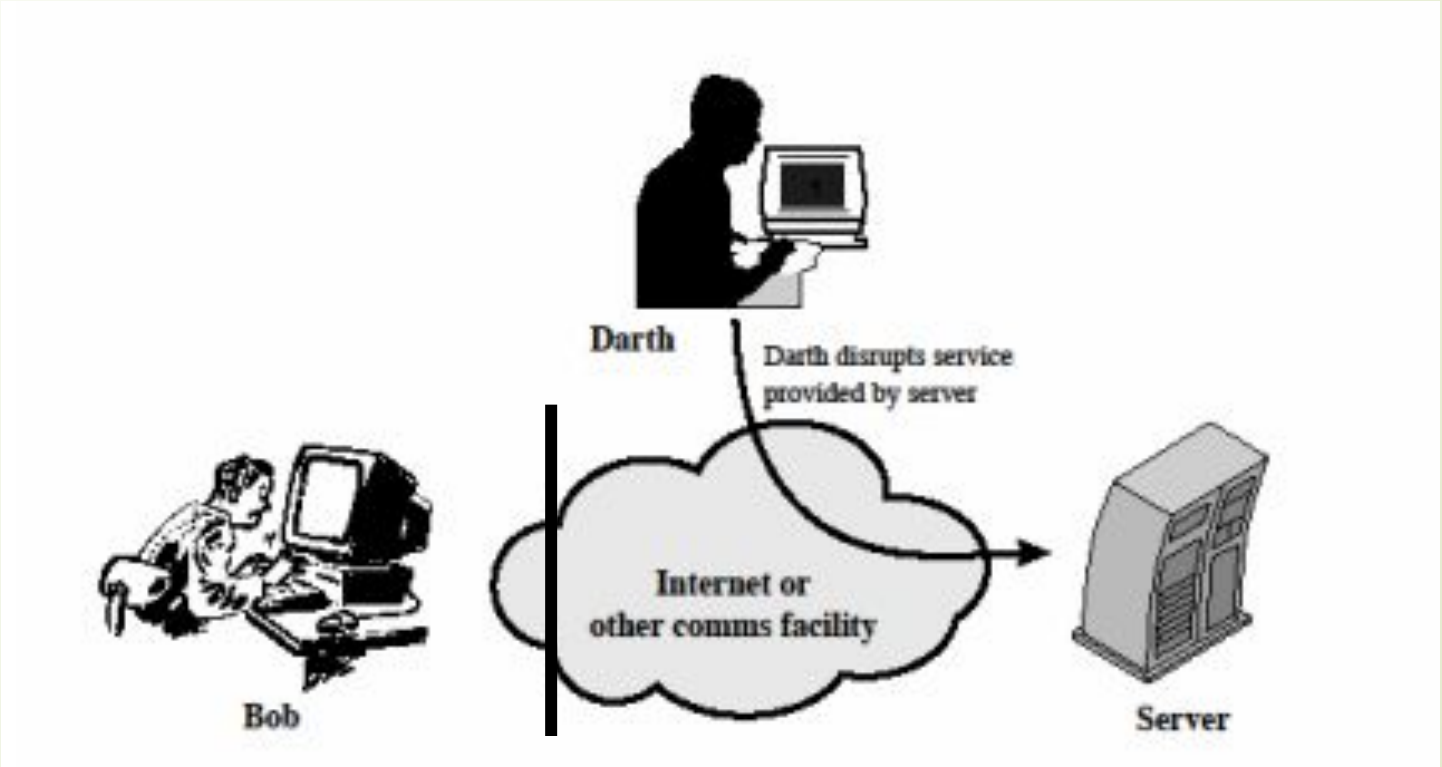
Repudiation

- It is **performed by one of the two parties in the communication**.
- The **sender of the message** might later **deny** that **she sent** the message.
- The **receiver of the message** might **later deny** that **he received** the message.

Denial of Service(Dos)



Active Attack
Denial of Services



Cryptology

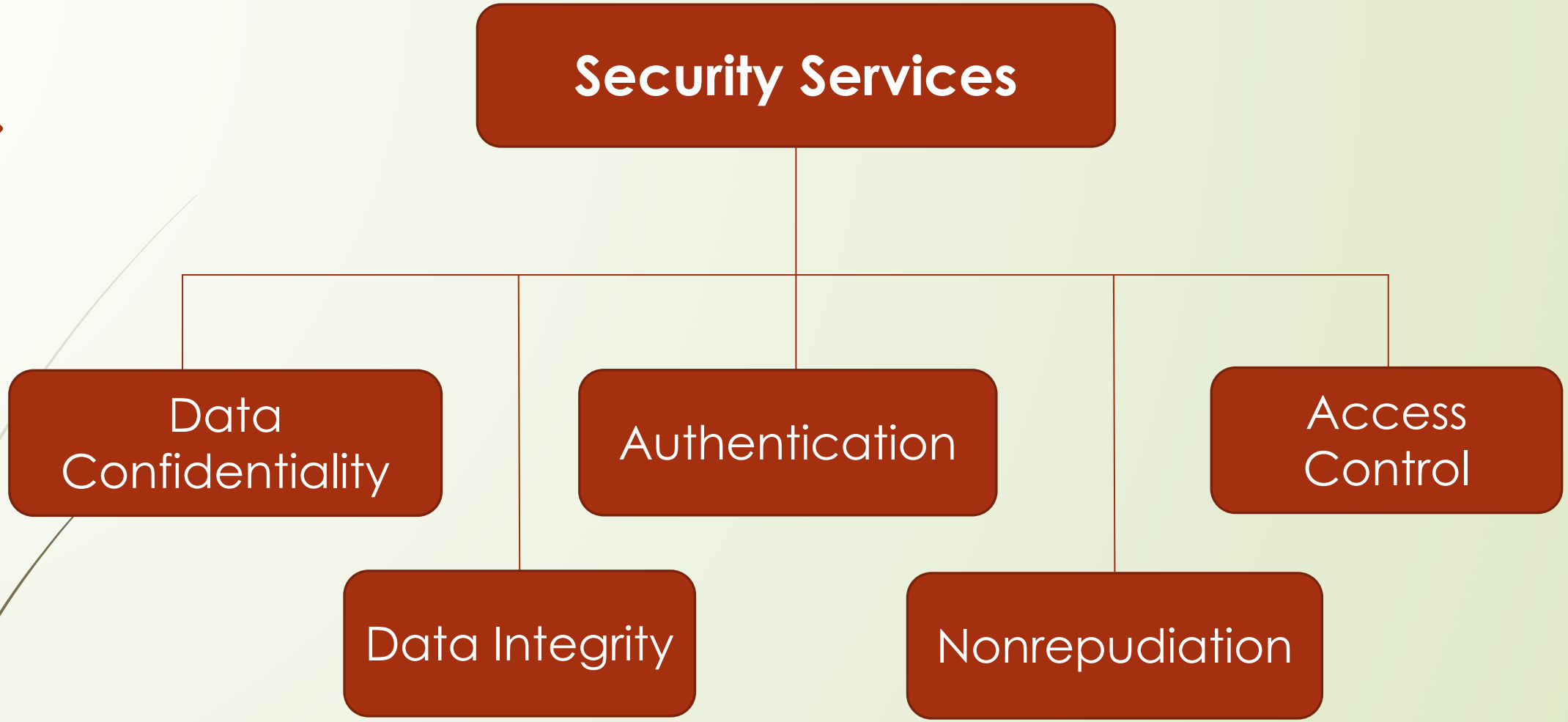
Cryptogrpahy

+

CryptAnalysis

Security Attack & Security Services

- **Security attack:** Any action that compromises the security of information owned by an organization.
- **Security service:** A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization.
- The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.



Enhances the security of the data processing systems and the information transfers of an organization.

Data Confidentiality

- Protection against passive attacks.
- Confidentiality **ensures** that **sensitive information** is **accessed only by an authorized person** and kept away from those not authorized to possess them.
- **Connection Confidentiality:** The protection of all user data on a connection.
- **Connectionless Confidentiality:** The protection of all user data in a single data block.
- **Selective-Field Confidentiality:** The confidentiality of selected fields within the user Data on a connection or in a single data block.
- **Traffic Flow Confidentiality:** The protection of the information that might be Derived from observation of traffic flows.

Examples of confidential information:

- Bank account statements
- Personal information
- Credit card numbers
- Trade secrets
- Government documents

Examples of attacks that affect confidentiality:

- Packet sniffing
- Password cracking
- Dumpster diving
- Wiretapping
- Keylogging
- Phishing

Ways to provide confidentiality:

- Usernames and passwords
- Two-factor authentication
- Biometric verification
- Security tokens or key fobs
- Data encryption

Authentication

- assures recipient that **the message is from the source** that it **claims to be** from.
- **For Connection Oriented communication**, authentication of sender and receiver is provided at the time of connection establishment which is known as **peer entity authentication.**
- Used in association with a logical connection to provide confidence in the identity of the entities connected.
- It attempts to provide confidence that an entity is not performing either a masquerade or an unauthorized replay of a previous connection.

Example: Entity authentication

- If you **log on to a computer system** there must (or at least should) be some way that you can convince it of your identity.
- Once it knows your identity, it can verify whether you are entitled to enter the system.
- The same principle applies when one person tries to communicate with another person: as a first step you want to verify that you are communicating with the right person.
- Therefore there must be some way in which you can prove your identity.

Continue…

- **For Connectionless Communication** , authentication of the source of the data is provided which is known as **data origin authentication.**
- It does not provide protection against the duplication or modification of data units.
- This type of service supports applications like electronic mail, where there are no prior interactions between the communicating entities.
- **Data authentication** consists of **two components:** the fact that **data has not been modified** (data integrity) and the fact that **you know who the sender is** (data origin authentication).

Ways to provide Authentication

- **a particular entity:** a password, a (pre-designed) user-id, a pin code, etc. **OR**
- **Another way is to use specific items to prove your identity:** a magnetic strip card, a smartcard (a hand-held computer the size of a credit card), a token. **OR**
- The two parties share **a common secret code** word. A party is required to **show the secret code word** to the other for **authentication**.)
- It is also possible to make **use of biometric properties. OR by sending digital signature**.
- **A trusted third party** verifies the authenticity. One such way is to use **digital certificates** issued by **a recognized certification authority**.

Access Control

- controls **who can have access** to a resource, **under what conditions** access can occur, and what those accessing the resource are
- While **authentication** can verify **the identity** of an entity, the **authorization** determines **what** the entity is **allowed to do.**
- **Authorization** is thus the act of **granting rights and/or privileges to users, permitting them access to an object**.
- **Access control** is a means of enforcing this authorization model. Usually a successful authentication is a must before the authorization of an action can be decided. allowed to do.

Data Integrity

- assurance that data received is as sent by an authorized entity.
- **Connection Integrity with Recovery:** Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.
- **Connection Integrity without Recovery:** As above, but provides only detection without recovery.
- **Selective-Field Connection Integrity:** Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.

Continue…

- **Connectionless Integrity:** Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.
- **Selective-Field Connectionless Integrity:** Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.

Nonrepudiation

- Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.
- **Nonrepudiation, Origin:** Proof that the message was sent by the specified party.
- **Nonrepudiation, Destination:** Proof that the message was received by the specified party.

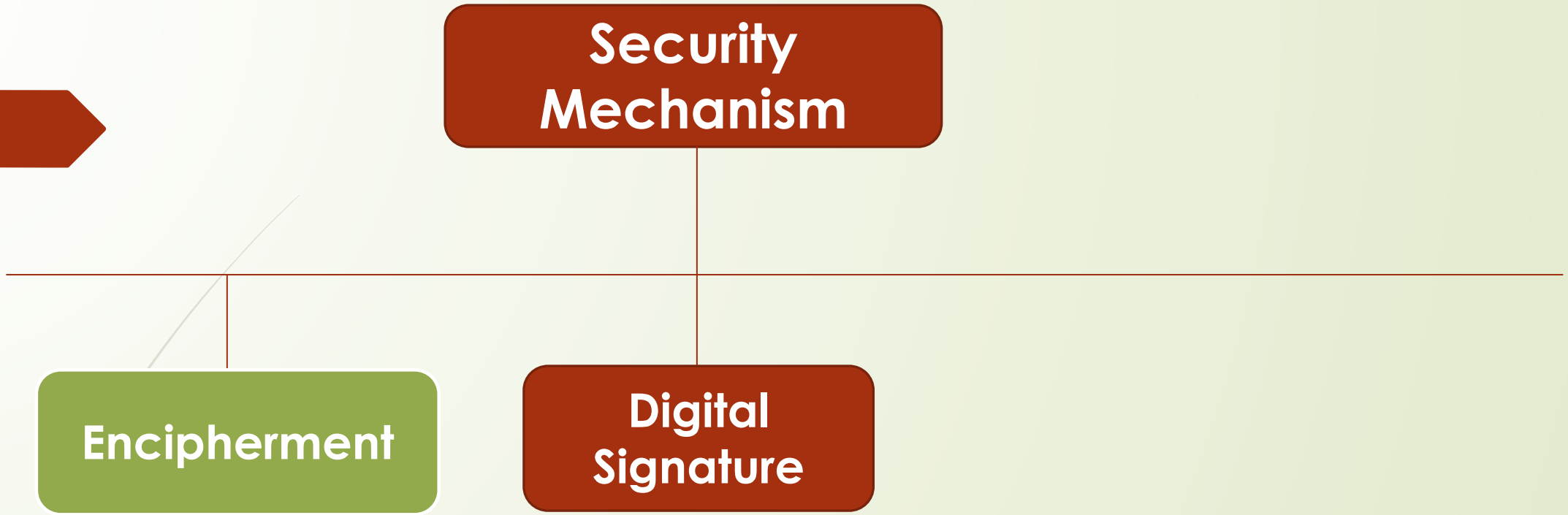
Security Mechanism

Digital Signature

A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.

Digital Signature

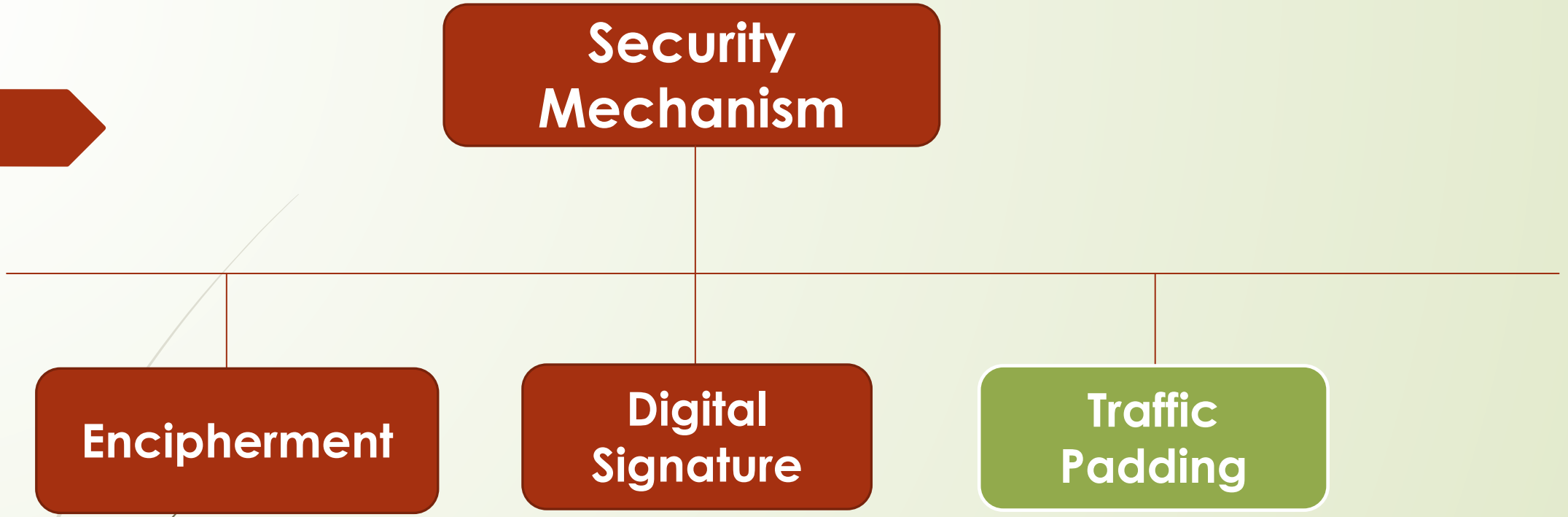
- **Data appended** to or a **cryptographic transformation of a data unit** that allows a recipient of the data unit to **prove the source and integrity of the data** unit and protect against forgery.



A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.

Encipherment

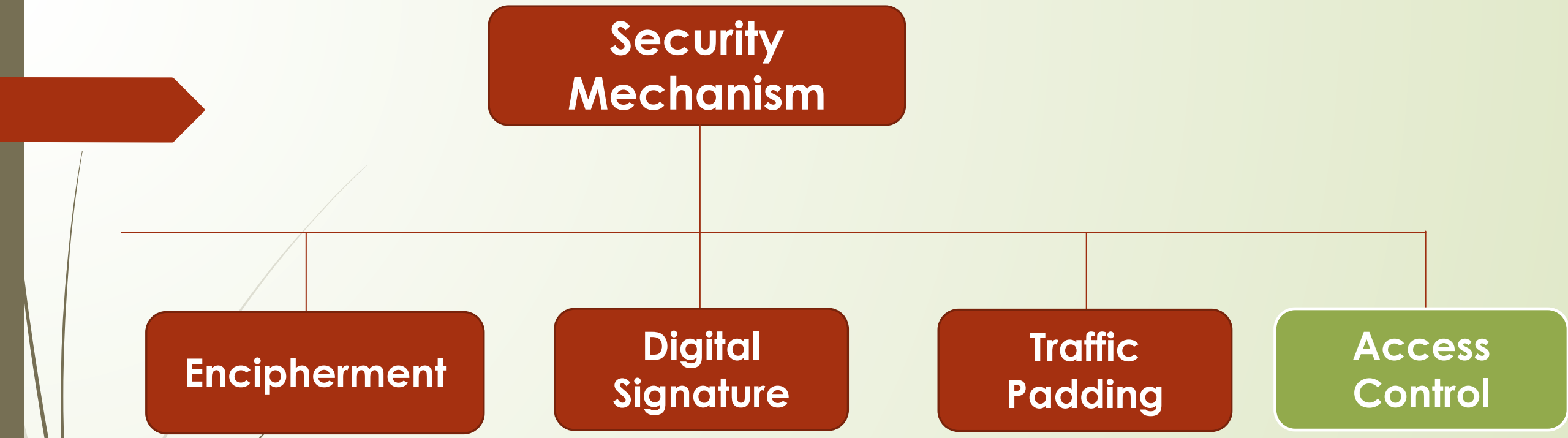
- **hiding or covering** of data which provides confidentiality.
- **Cryptography and Steganography** are used for enciphering.



A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.

Traffic Padding

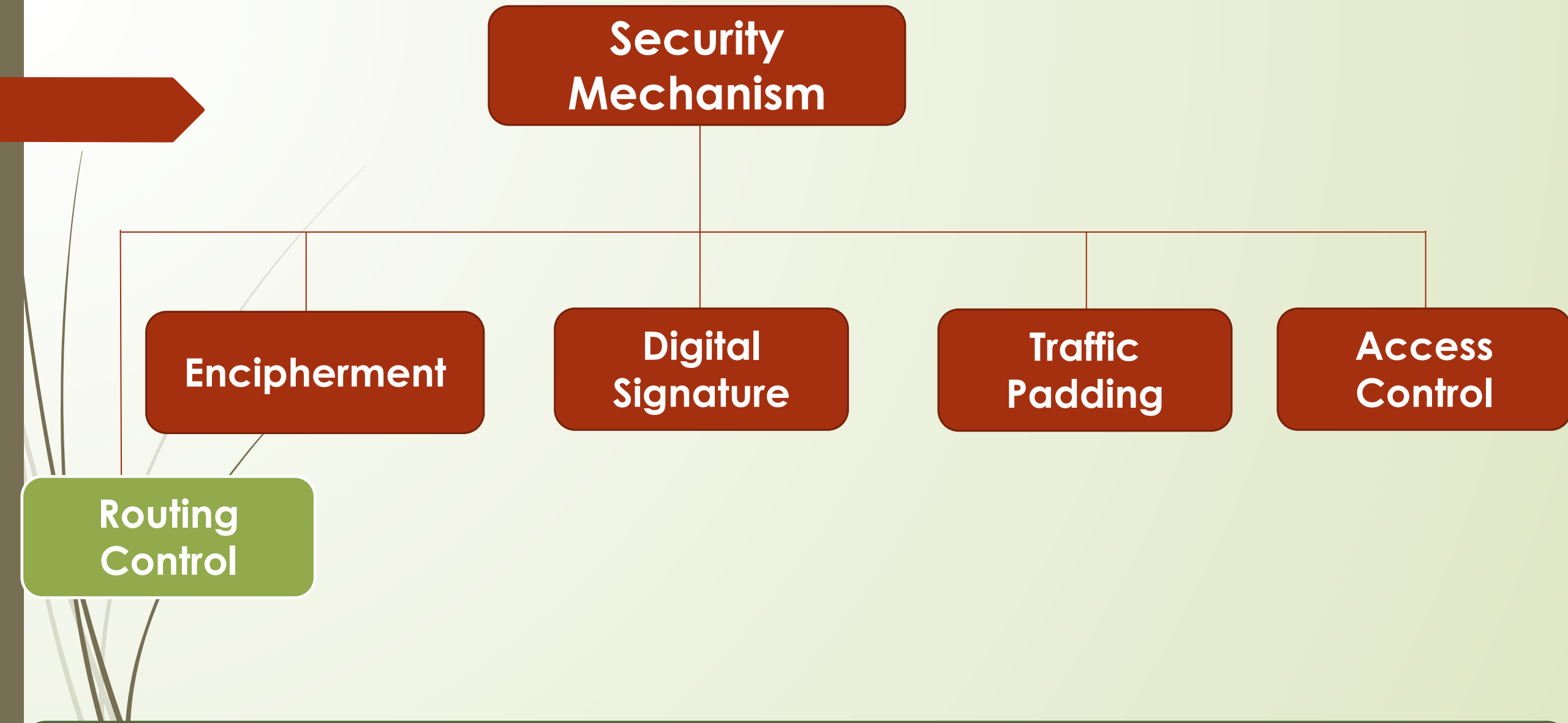
- inserting some bogus data into the data traffic to **thwart the adversary's attempt** to use the **traffic analysis**
- The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.



A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.

Access Control

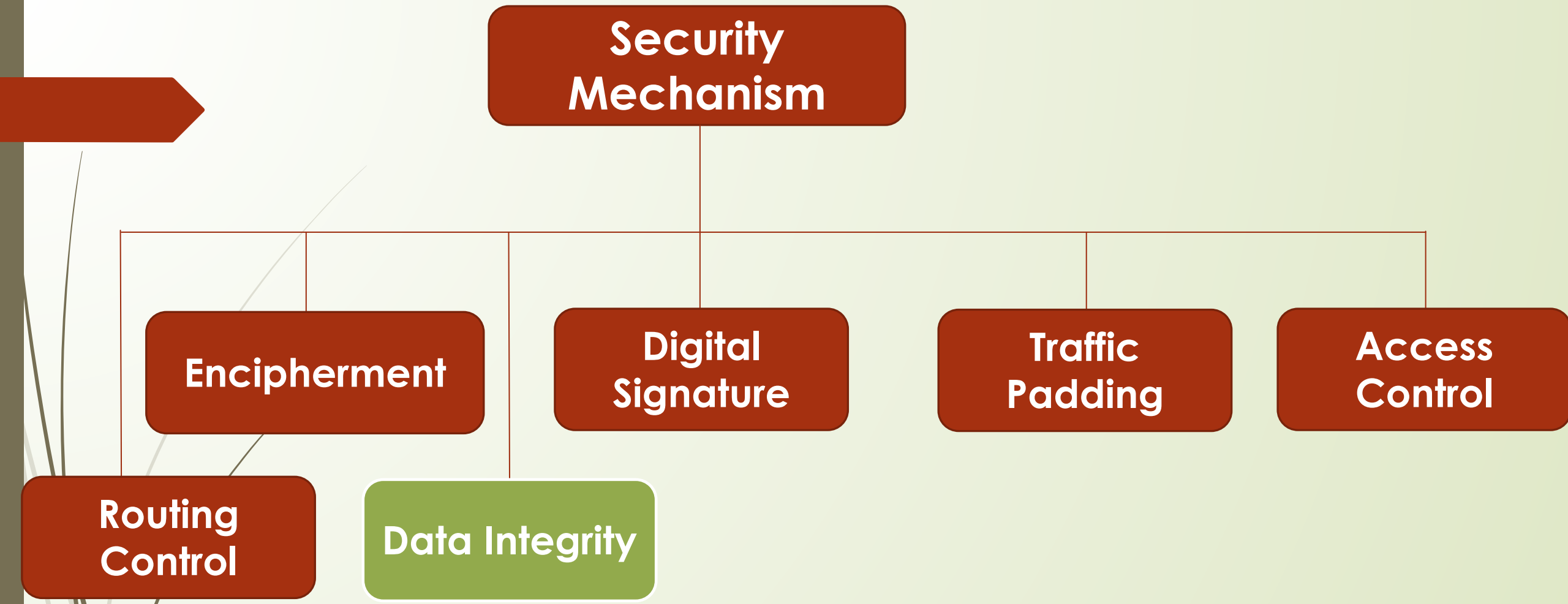
- A **variety of mechanisms** that **enforce access rights** to resources.
- Access control used **methods to prove** that a **user has access right** to the **data or resources** owned by a system.
- Examples of proofs are passwords and PINs.



A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.

Routing Control

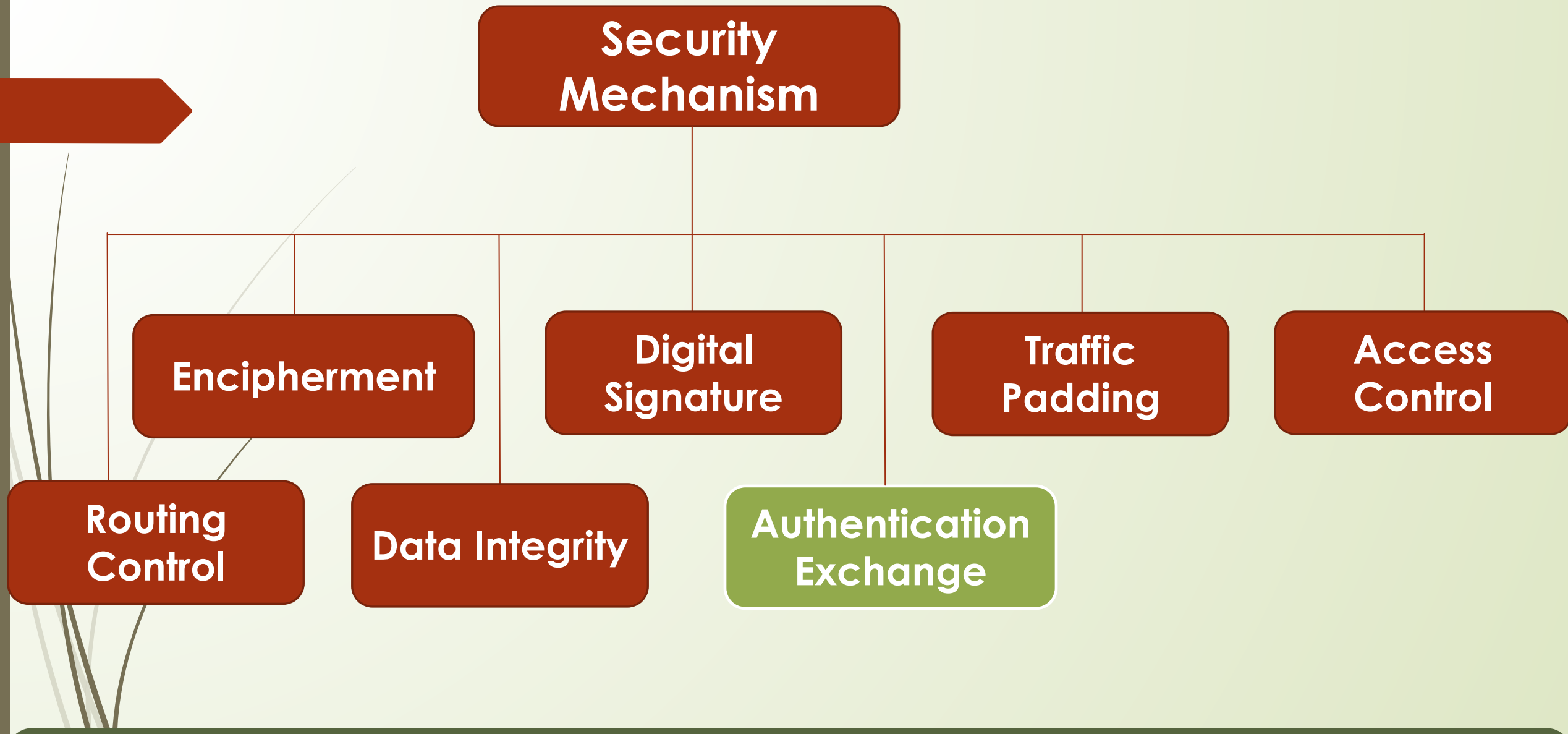
- Routing control means **selecting and continuously changing** different **available routes between sender and receiver** to prevent the opponent from eavesdropping on a particular route.
- Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.



A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.

Data Integrity

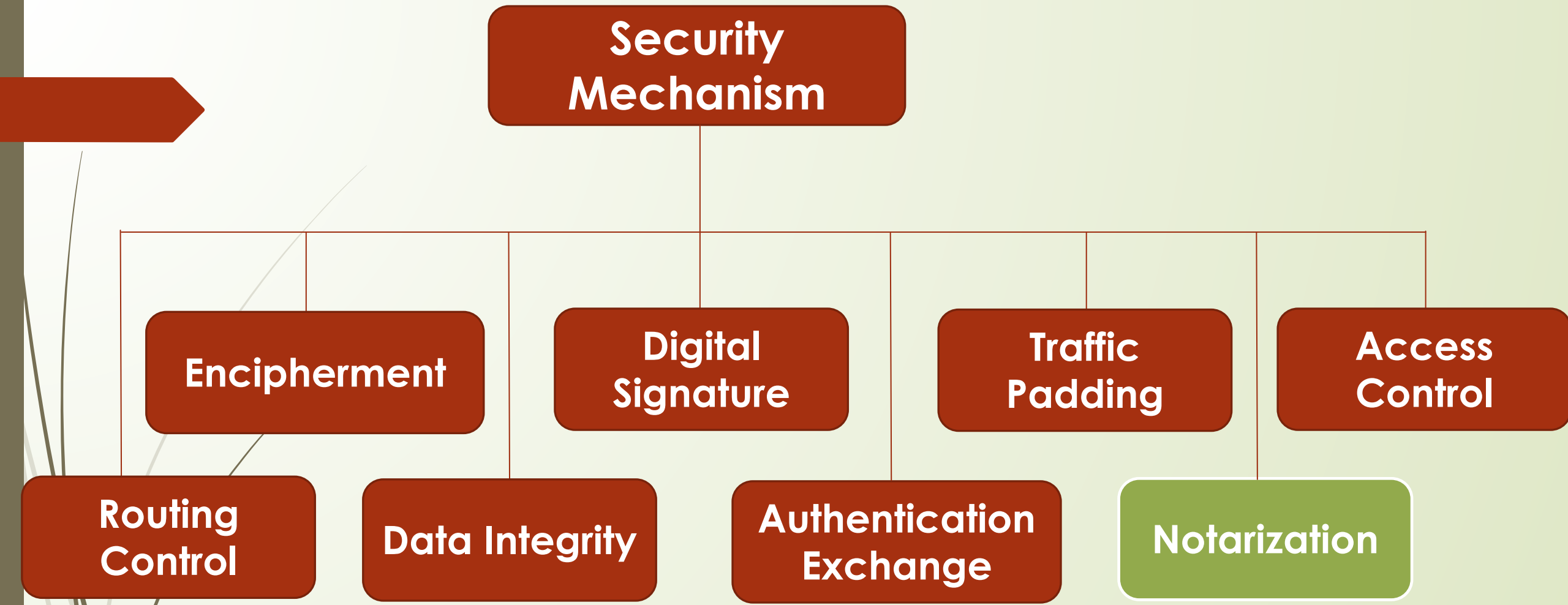
- A variety of mechanisms used to assure the integrity of a data unit or stream of data units.
- The data integrity mechanism **appends** to the data **a short check value** that has been **created** by a specific process **from the data itself**.
- **Data integrity** is preserved by **comparing check value received** to the check value generated.



A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.

Authentication Exchange

- In this two entities **exchange some messages** to **prove their identity** to each other.



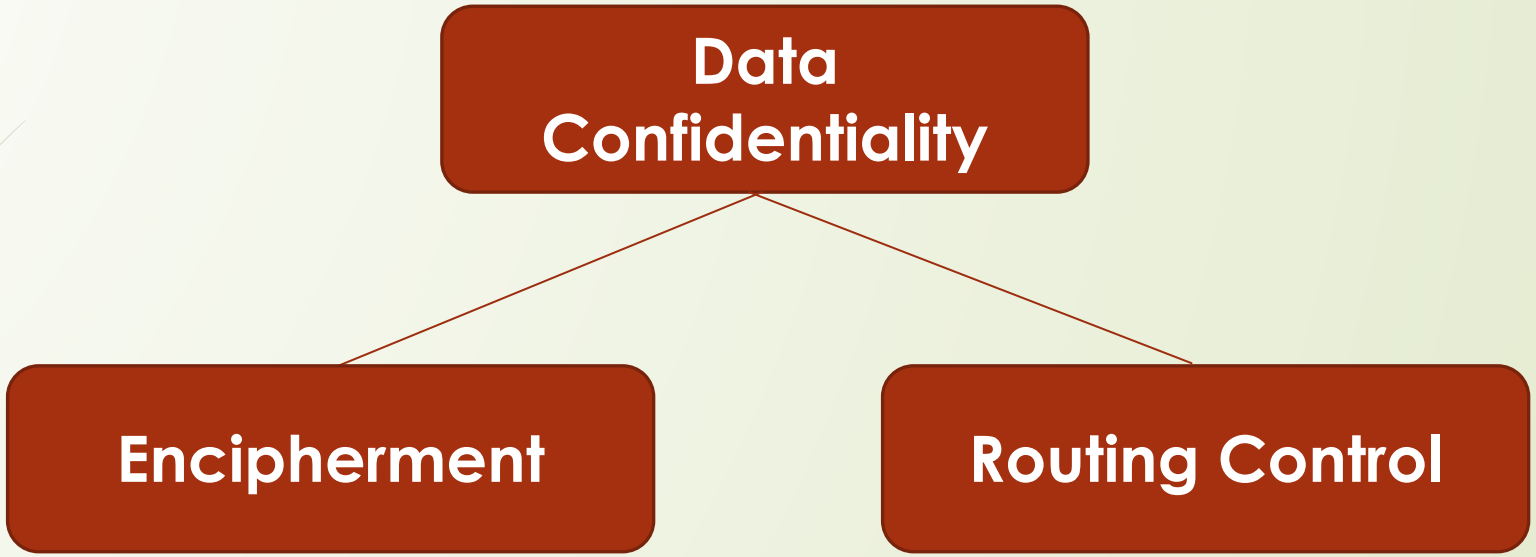
A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.

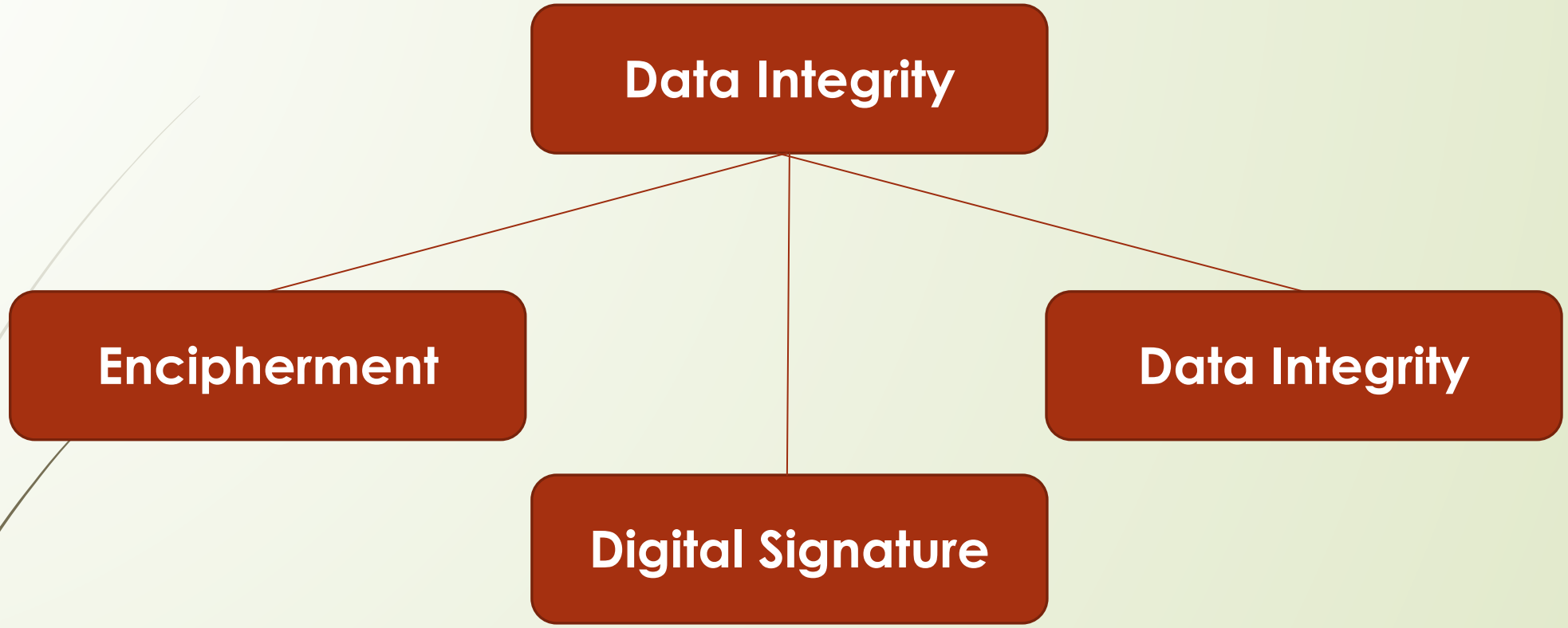
Notarization

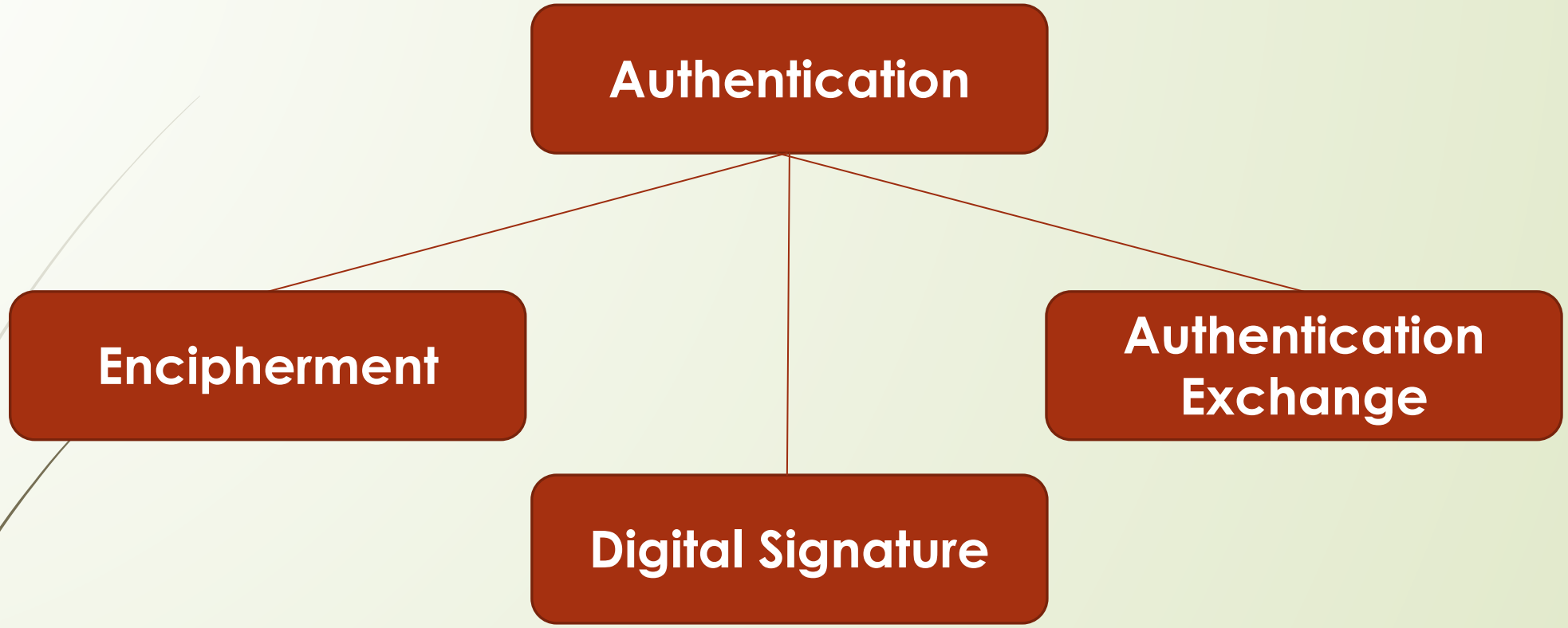
- The use of a **trusted third party** to assure certain properties of a data exchange.
- **A third trusted party** to **control** the **communication between two entities**.
- **The receiver can involve** a trusted third party to store the sender request in order to prevent the sender from later denying that she has made a request.

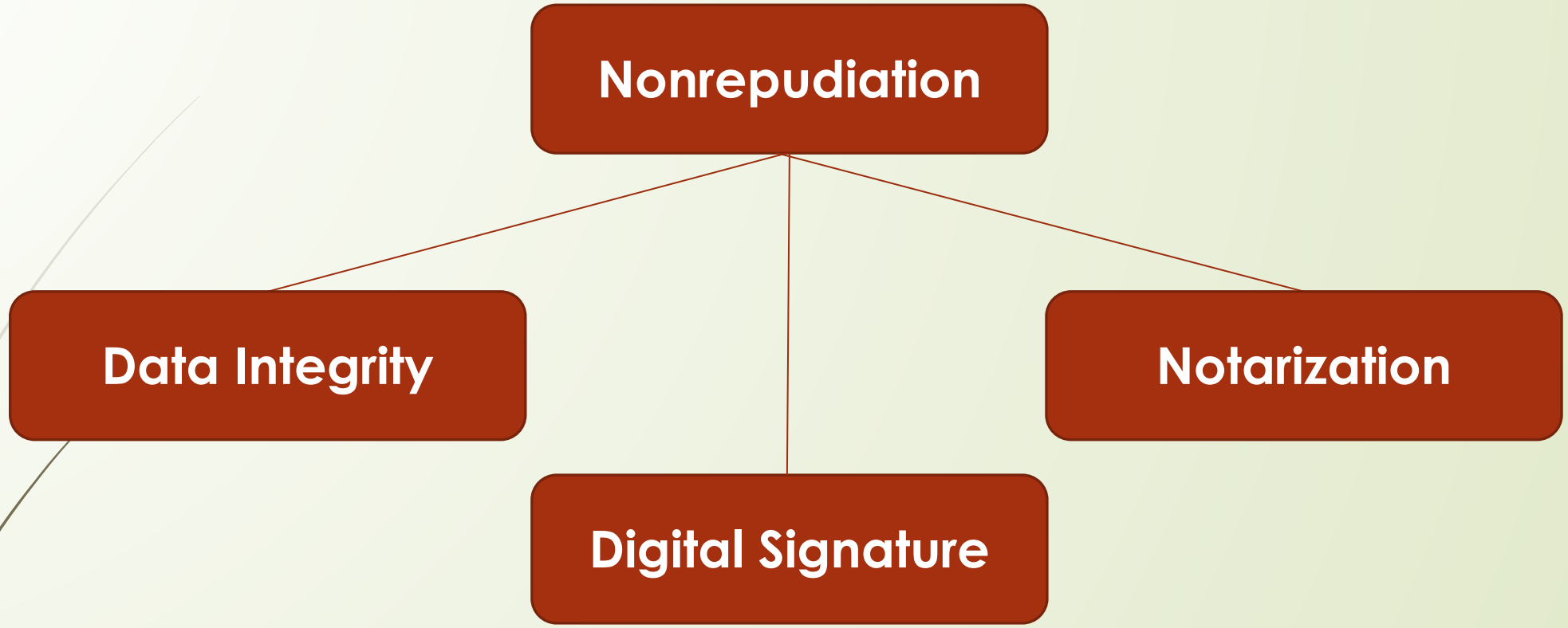
Relation between Services and Mechanisms

- **Security services** and **mechanisms** are **closely related** as **mechanisms** and **combination of mechanisms** are used to **provide a service**.


Data Confidentiality
Encipherment
Routing Control


Data Integrity
Encipherment
Digital Signature
Data Integrity


Authentication
Encipherment
Digital Signature
Authentication Exchange


Nonrepudiation
Data Integrity
Digital Signature
Notarization

Mechanism								
Service	Encipherment	Digital Signature	Access Control	Data Integrity	Authentication Exchange	Traffic Padding	Routing Control	Notarization
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

Exercise

- Draw a matrix that shows the relationship between security services and attacks.
- Solution
- Draw a matrix that shows the relationship between security mechanisms and attacks.
- Solution

- Which security mechanism(s) are provided in each of the following cases?

1. A School demands student identification and a password to let students log into the school server.
2. A school server disconnects a student if she logged into the system for more than two hours.
3. A professor refuses to send students grades by email unless they provide student identification they were pre assigned by the professor.
4. A bank requires the customer's signature for a withdrawal.

Any Questions??

Thank You

Answers

	Release of message contents	Traffic analysis	Masquerade	Replay	Modification of messages	Denial of service
Peer entity authentication			Y			
Data origin authentication			Y			
Access control			Y			
Confidentiality	Y					
Traffic flow confidentiality		Y				
Data integrity				Y	Y	
Non-repudiation			Y			
Availability						Y

	Release of message contents	Traffic analysis	Masquerade	Replay	Modification of messages	Denial of service
Encipherment	Y					
Digital signature			Y	Y	Y	
Access control	Y	Y	Y	Y		Y
Data integrity				Y	Y	
Authentication exchange	Y		Y	Y		Y
Traffic padding		Y				
Routing control	Y	Y				Y
Notarization			Y	Y	Y	